Understand DNS and SWG Backoff Settings for CSC

Contents

Introduction

This document describes DNS and Secure Web Gateway (SWG) Backoff Settings for Cisco Secure Client (CSC).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Secure Client.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

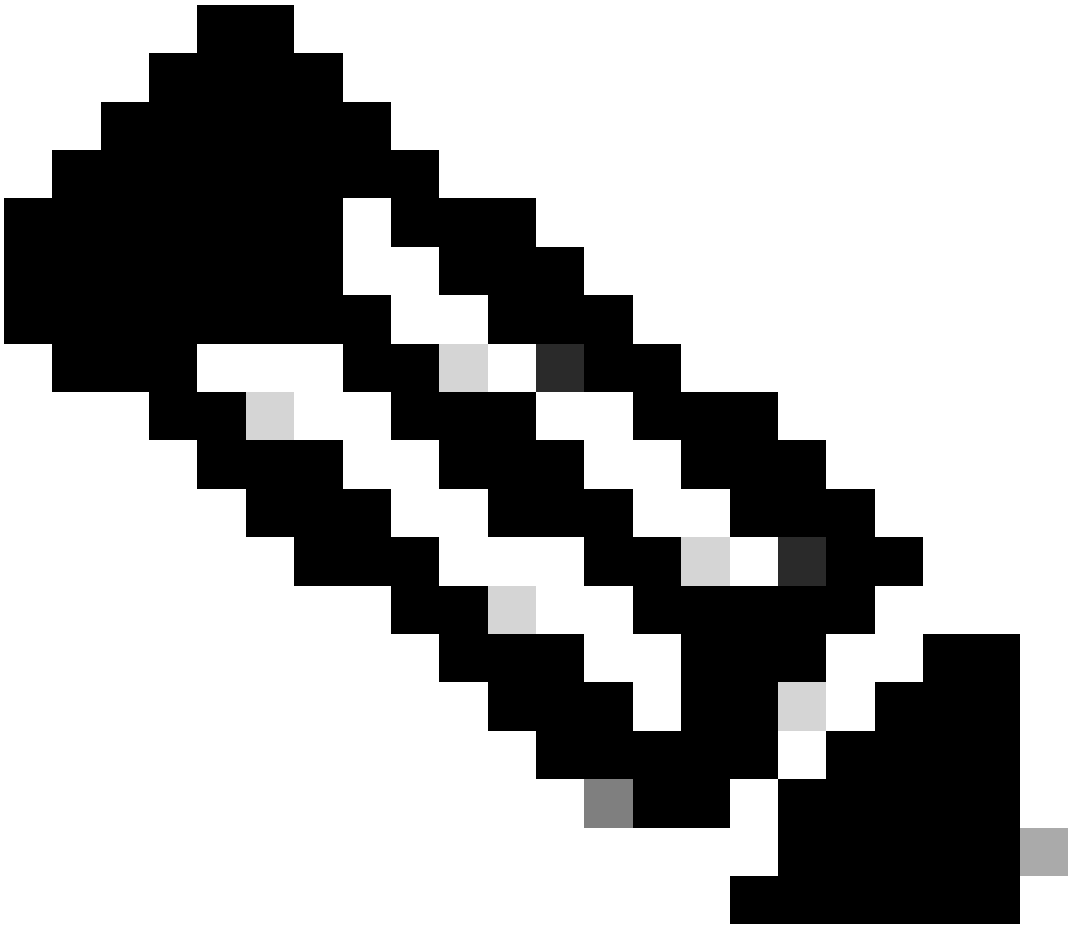
Until around April 25, 2024, the Cisco Secure Client's SWG module backoff behavior was not able to be controlled irrespective of the DNS module's state and was dependent on the DNS backoff settings to enable/disable SWG protection. To address this, Umbrella has decoupled the behavior for the DNS module and the SWG module, enabling independent management as needed. This is available to **Cisco Secure Clients on version 5.1.3.62 and newer** where Umbrella decoupled the DNS and SWG backoff settings to allow for enhanced granular control. Clients on older versions did not follow the separate SWG module backoff.

When the **Secure Web Gateway backoff follows DNS backoff** feature is enabled, the CSC's SWG module follows the behavior of the DNS module. However, this does not occur with all DNS backoff settings. In the next section, the DNS backoff settings that the SWG module do or do not follow are detailed.

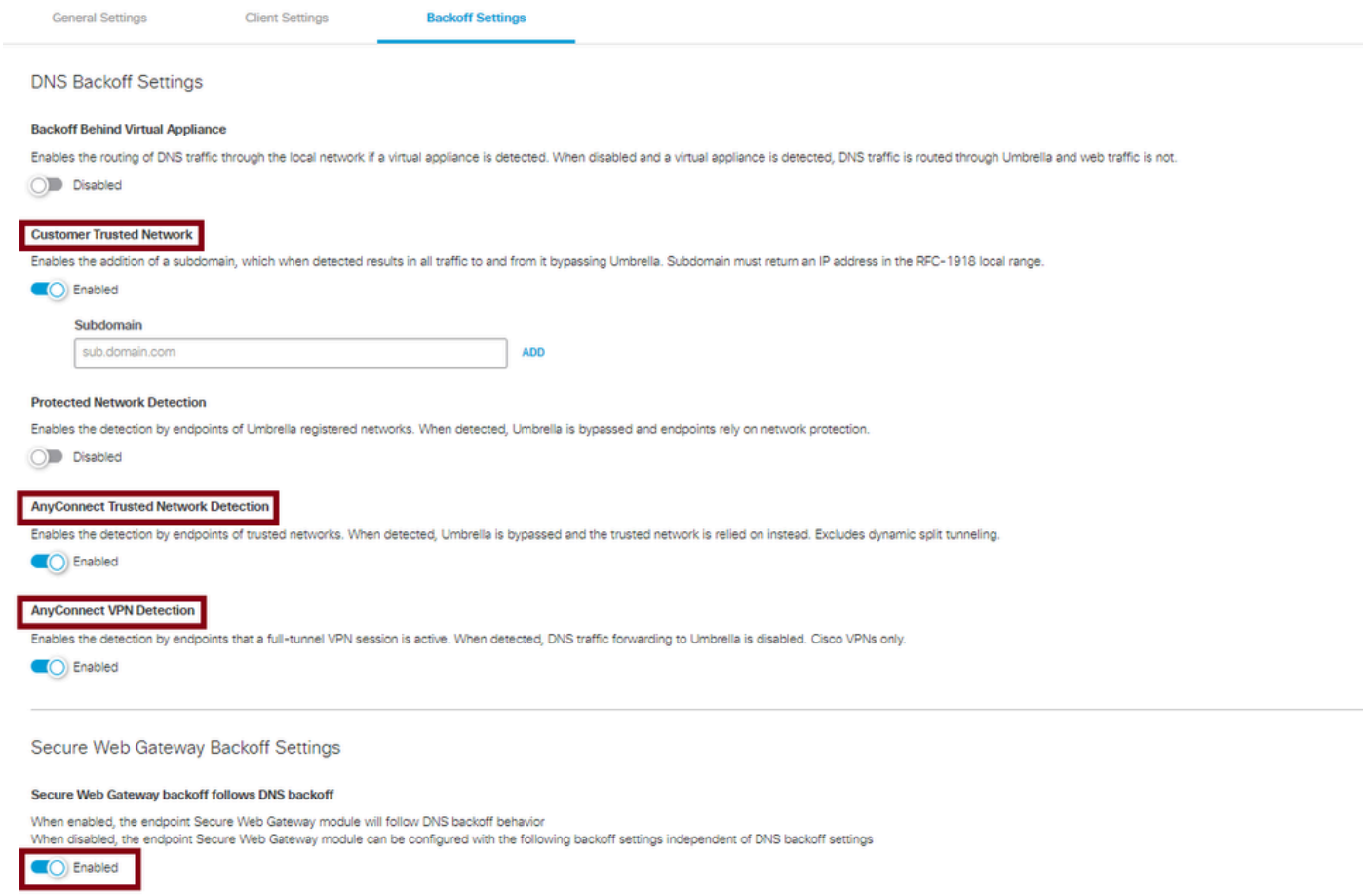
Which DNS Backoff Settings Cause SWG to Back Off?

These DNS backoff settings cause SWG to backoff:

- Customer Trusted Network: Setting up a **Customer Trusted Network** domain in the DNS backoff settings is one of the simplest methods. By hosting an internal domain that resolves to an RFC1918 address, both DNS and SWG can simultaneously backoff. Umbrella's client is coded to query that domain. If it successfully resolves the domain to a private IP address, it identifies the device as being on a private and protected network, causing the DNS module to back off. This backoff mechanism is also respected by the Web module, which can similarly back off when the DNS module successfully resolves the domain.
- AnyConnect Trusted Network Detection
- AnyConnect VPN Detection



Note: The DNS backoff settings remain functional on **Cisco Secure Clients running versions older than 5.1.3.62**, as it was implemented prior to the decoupling of the DNS and SWG backoff settings.

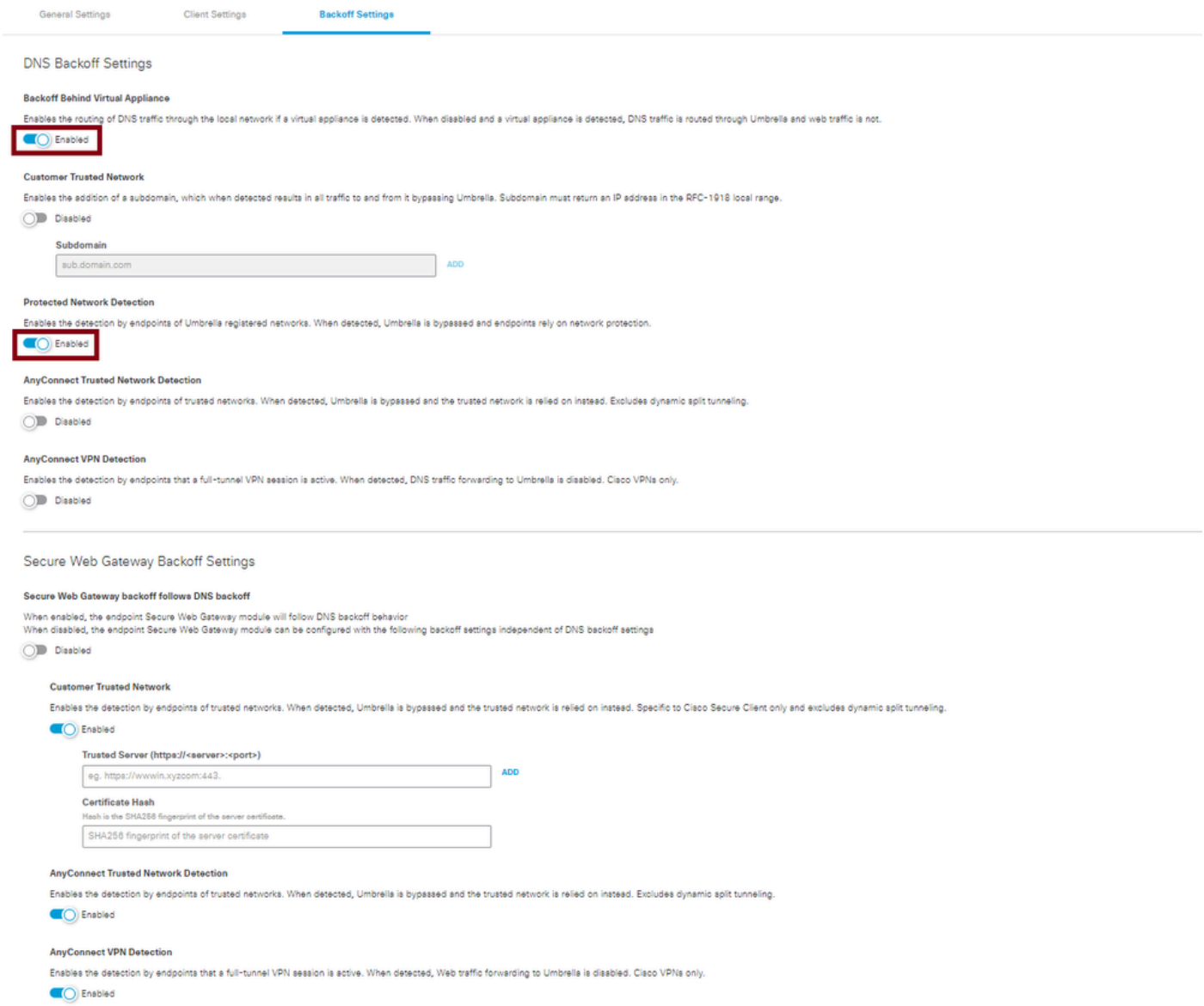


27885424859028

Which DNS Backoff Settings Do Not Cause SWG to Back Off?

Configuring these two DNS backoff features does not cause SWG to back off. Therefore, you must configure SWG backoff settings selectively, independent of the DNS configuration state. This is discussed in more detail in the next section.

- Backoff Behind Virtual Appliance: Starting from AnyConnect 4.10.07061 (MR7) and Secure Client 5.0.02075 (MR2), the SWG module can remain enabled on networks where an Umbrella virtual appliance is present. If you were previously relying on the presence of a virtual appliance to disable the SWG module and web redirection on a given network, you can instead use Trusted Network Domain or AnyConnect Trusted Network Detection.
- Protected Network Detection



27885587178772

Independent SWG Backoff Settings

If these DNS backoff features are not enabled in your environment, you can exclusively utilize one of the SWG backoff settings outlined here to ensure SWG remains disabled:

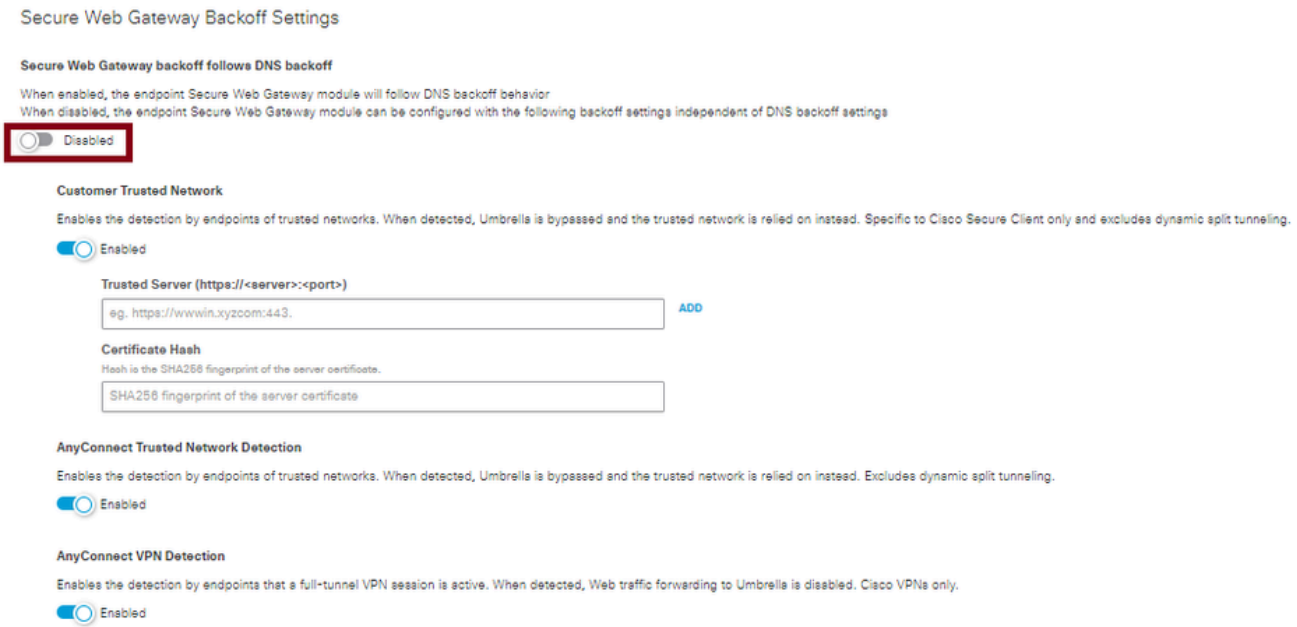
- Customer Trusted Network
- AnyConnect Trusted Network Detection
- AnyConnect VPN Detection

This new capability allows the SWG module to operate independently of the DNS module. **This feature is available to Cisco Secure Clients using version 5.1.3.62 and newer**. Configure one of the explicit SWG backoff toggles in the dashboard:

- Customer Trusted Network: One option is to use the **Customer Trusted Network** option under the SWG backoff settings where you can configure an internal server that the client can reach out to confirm that it is on the protected network. You need to ensure the web server is reachable by the client, obtain a certificate on that server, and copy the certificate hash to the Umbrella dashboard.

The other two options apply exclusively to VPN connections:

- AnyConnect Trusted Network Detection
- AnyConnect VPN Detection



27886005743764